UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/772,433	02/06/2004	Marcus Leech	57983.000164	5978

7590 01/07/2008

Thomas E. Anderson
Hunton & Williams LLP
1900 K Street, N.W.
Washington, DC 20006-1109

EXAMINER	
LANIER, BENJAMIN E	

ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
01/07/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

AK

Advisory Action ***Before the Filing of an Appeal Brief***	**Application No.** *10/772,433*	**Applicant(s)** LEECH, MARCUS	
	Examiner Benjamin E. Lanier	**Art Unit** 2132	

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 19 December 2007 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. ☒ The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:

   a) □ The period for reply expires ______months from the mailing date of the final rejection.

   b) ☒ The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

   Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. □ The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. ☒ The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because

   (a) ☒ They raise new issues that would require further consideration and/or search (see NOTE below);

   (b) □ They raise the issue of new matter (see NOTE below);

   (c) □ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or

   (d) □ They present additional claims without canceling a corresponding number of finally rejected claims.

   NOTE: *See Continuation Sheet*. (See 37 CFR 1.116 and 41.33(a)).

4. □ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).

5. □ Applicant's reply has overcome the following rejection(s): _____.

6. □ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).

7. □ For purposes of appeal, the proposed amendment(s): a) □ will not be entered, or b) □ will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.

   The status of the claim(s) is (or will be) as follows:

   Claim(s) allowed: _____.

   Claim(s) objected to: _____.

   Claim(s) rejected: _____.

   Claim(s) withdrawn from consideration: _____.

AFFIDAVIT OR OTHER EVIDENCE

8. □ The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).

9. □ The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing a good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).

10. □ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. ☒ The request for reconsideration has been considered but does NOT place the application in condition for allowance because: See Continuation Sheet.

12. □ Note the attached Information Disclosure Statement(s). (PTO/SB/08) Paper No(s). _____

13. □ Other: _____.

Benjamin E. Lanier
Primary Examiner
AU 2132

Continuation of 3. NOTE: Claim 1 as amended changes the scope of claims 6-9, and 11 because claim 1 was amended to include limitations from claim 2. Claims 6-9, and 11 depend from claim 1 and therefore, the limitaitons of claim 2 have not been considered with respect to claims 6-9 and 11.

Continuation of 11. does NOT place the application in condition for allowance because: Applicant argues, "Rogaway fails to disclose or even suggest the elements of applying a XOR function to all blocks of a message to compute a XOR-sum, applying a first mask value to the XOR-sum, encrypting the masked XOR-sum using a block cipher and a first key, and applying a second mask value to the encrypted XOR-sum to generate an integrity tag, as claimed." This argument is not persuasive because Rogaway discloses that each message blocks is concatenated (Page 5, checksum generation function), which meets the limitation of applying a XOR function to all message blocks of a message to compute a XOR-sum. The checksum is then XOR'd with Z[m] (Page 5, calculation of value 'T'), which meets the limitation of applying a third mask value to the XOR-sum. The result of the XOR function is then encrypted (Page 5, calculation of value 'T'), which meets the limitation of encrypting the masked XOR-sum using the block cipher and the first key. Rogaway does not disclose XOR'ing the result of the encryption with a value. However, it would have been obvious to one of ordinary skill in the art at the time the invention was made to XOR the data after the block algorithm, in addition to before, because this technique is not susceptible to meet-in-the-middle attack as taught by Schneier (Page 367).
Applicant argues, "Rogaway also discloses applying a string L and an offset Z[m] to one string of a message M before a block cipher Ek, as well as applying the same message string M[m] after the block cipher Ek (see pages 4-6)." Applicant has not considered the proposed modification of Rogaway used to rejection claim 12, which suggests that it would have been obvious to one of ordinary skill in the art at the time the invention was made to XOR the data after the block algorithm, in addition to before, because this technique is not susceptible to meet-in-the-middle attack as taught by Schneier (Page 367).
Applicant argues, "Rogaway also discloses applying and limiting as described above to a checksum of xor'ed message strings M, cyphertext string C[m], and block ciphered string Y[m]." Applicant appears to have not considered the entire rejection, as mentioned above. Rogaway teaches applying a XOR function to all blocks of a message to compute a XOR-sum (See page 5, calculation of Checksum), applying a first mask value to the XOR-sum (See page 5, Checksum Z[m]), encrypting the masked XOR-sum using a block cipher and a first key (See page 5, Ek(Checksum Z[m]). Rogaway does not disclose XOR'ing the result of the encryption with a value. However, it would have been obvious to one of ordinary skill in the art at the time the invention was made to XOR the data after the block algorithm, in addition to before, because this technique is not susceptible to meet-in-the-middle attack as taught by Schneier (Page 367)..

Applicant argues, "Regarding combining Schneier with Rogaway to arrive at the claimed invention, such a combination would result in an inoperable methodology since replacing the limiting of Rogaway with an additional xor function as mentioned by Schneier would not result in a limited tag length τ, which is required by Rogaway." This argument is not persuasive because the proposed modification of Rogaway never alleged "replacing the limiting of Rogaway with an additional xor function" as alleged by Applicant, but instead suggested exclusive or'ing the result of encrypting (Checksum Z[m]). Additionally, Applicant's allegation of inoperability is unsupported by any actual cited evidence and is therefore unpersuasive.